

UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina



Farhad Azima

Plaintiff

v.

Nicholas Del Rosso & Vital Management Services, Inc

Defendant

Civil Action No. 20-cv-954

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS
OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To:

Craig Thomas Evers, 7507 Kilcullen Drive, Charlotte, NC 28270

(Name of person to whom this subpoena is directed)

☒ **Production:** YOU ARE COMMANDED to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material:

See Attachment A.

Place: Womble Bond Dickinson (US) LLP
301 S. College Street #3500, Charlotte, NC 28202
Consent to Remote Compliance.

Date and Time:

04/07/2023 5:00 pm

☐ **Inspection of Premises:** YOU ARE COMMANDED to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:

Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 03/23/2023

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

Attorney's signature Calvin Lee

The name, address, e-mail address, and telephone number of the attorney representing (name of party) Farhad Azima
Calvin Lee, Miller & Chevalier Chartered, who issues or requests this subpoena, are:
900 16th Street NW, Washington, DC 20006, (202) 626-5981, clee@milchev.com

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

EXHIBIT A

Civil Action No. 20-cv-954

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____
on *(date)* _____.

☐ I served the subpoena by delivering a copy to the named person as follows: _____

_____ on *(date)* _____; or

☐ I returned the subpoena unexecuted because: _____

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also
tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of
\$ _____.

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) For a Trial, Hearing, or Deposition. A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

- (A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or
- (B) within the state where the person resides, is employed, or regularly transacts business in person, if the person
 - (i) is a party or a party's officer; or
 - (ii) is commanded to attend a trial and would not incur substantial expense.

(2) For Other Discovery. A subpoena may command:

- (A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and
- (B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) Avoiding Undue Burden or Expense; Sanctions. A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) Command to Produce Materials or Permit Inspection.

(A) Appearance Not Required. A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) Objections. A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

- (i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.
- (ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) Quashing or Modifying a Subpoena.

(A) When Required. On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

- (i) fails to allow a reasonable time to comply;
- (ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);
- (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or
- (iv) subjects a person to undue burden.

(B) When Permitted. To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

- (i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) Specifying Conditions as an Alternative. In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

- (i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and
- (ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) Producing Documents or Electronically Stored Information. These procedures apply to producing documents or electronically stored information:

(A) Documents. A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) Form for Producing Electronically Stored Information Not Specified. If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) Electronically Stored Information Produced in Only One Form. The person responding need not produce the same electronically stored information in more than one form.

(D) Inaccessible Electronically Stored Information. The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) Claiming Privilege or Protection.

(A) Information Withheld. A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

- (i) expressly make the claim; and
- (ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) Information Produced. If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

Attachment A

INSTRUCTIONS

1. Prior to answering the following, you are requested to make a due and diligent search of your books, records, and papers, with a view to eliciting all information responsive to this subpoena.

2. If you object to any request on the basis of privilege, please identify the nature of the documents being withheld on that basis.

3. If any document responsive to this request was, but no longer is in your possession, state whether it is missing or lost; if it has been destroyed; if it has been transferred, voluntarily or involuntarily, to others; or if it has otherwise been disposed of. In each instance, identify the document fully, explain the circumstances, and identify the people having knowledge of such circumstances.

4. If you contend that any documents covered in these requests are not reasonably accessible or would be unduly burdensome to locate or produce, identify such documents by category and source and provide detailed information regarding the burden or cost you claim is associated with the search for or production of such documents.

5. To the extent documents produced in response to this request include electronic documents, such as spreadsheets or databases, please produce all such documents in native form, ensuring that all formulae and metadata embedded in such documents are produced.

6. To the extent you intend to not produce a requested document, you are directed to make and safeguard a copy of the requested information.

7. The relevant time period for documents responsive to the following requests shall be between August 1, 2014 until now.

DEFINITIONS

1. The term "Communication" means any oral, written, or electronic transmission of information, including but not limited to records of face-to-face meetings, letters, emails, text messages, messaging applications, social media messaging, telephone calls, chat rooms, or group list serves.

2. The term "Document" is intended to be as comprehensive as the meaning provided in Rule 34 of the Federal Rules of Civil Procedure.

3. The term “Person” means any individual, corporation, partnership, proprietorship, association, organization, governmental entity, group of persons or any other entity of whatever nature.

4. The terms “relate to” or “relating to” means consisting of, referring to, regarding, reflecting, supporting, prepared in connection with, used in preparation of, or being in any way logically or factually connected with the matter discussed.

5. The term “you” means Craig Thomas Evers, former associate of Vital Management Services, Inc and Nicholas Del Rosso.

6. “Plaintiff” refers to Farhad Azima, the plaintiff in this action.

7. “Defendants” refers to Nicholas Del Rosso and Vital Management Services, Inc.

8. “Nicholas Del Rosso” refers to Nicholas Del Rosso, the owner and an employee of the company Vital Management Services, Inc. Del Rosso is believed to reside at 318 Lystra Preserve Drive, Chapel Hill, North Carolina 27517.

9. “Vital Management Services, Inc.” and “Vital” refer to a company believed to be owned and operated by Nicholas Del Rosso located at 1340 Environ Way, Chapel Hill, North Carolina, 27517.

10. “Hacked Data” refers to any data belonging to Plaintiff that came into Defendants’ possession or your possession without consent from Plaintiff.

11. “CyberRoot” refers to CyberRoot Risk Advisory Private Limited and all current and former employees, agents, representatives, subsidiaries, affiliates, assignees, or other persons acting or purporting to act on its behalf.

12. “BellTroX” refers to BellTroX Info Tech Services and all employees, agents, representatives, subsidiaries, affiliates, assignees, or other persons acting or purporting to act on its behalf.

13. “Aditya Jain” refers to the founder, owner, manager, or principal of the following companies: (1) Cyber Defense and Analytics; (2) WhiteInt Consulting Pvt Ltd; (3) Cyber DNA Labs (OPC) Pvt Ltd; and (4) Arceus Consulting LLP.

14. “Jain Entities” refers to Cyber DNA, WhiteInt, Arceus, and any other company for which Aditya Jain is an authorized signatory or owner.

15. “Cyber DNA” refers to Cyber Defence and Analytics and all employees, agents, representatives, subsidiaries, affiliates, assignees, or other persons acting or purporting to act on its behalf, including but not limited to Aditya Jain.

16. “Cyber DNA Labs” refers to Cyber DNA Labs (OPC) Pvt Ltd and all employees, agents, representatives, subsidiaries, affiliates, assignees, or other persons acting or purporting to act on its behalf, including but not limited to Aditya Jain.

17. “WhiteInt” refers to a company owned by Aditya Jain including all employees, agents, representatives, subsidiaries, affiliates, assignees, or other persons acting or purporting to act on its behalf, including but not limited to Aditya Jain.

18. “Arceus” refers to a company owned by Aditya Jain including all employees, agents, representatives, subsidiaries, affiliates, assignees, or other persons acting or purporting to act on its behalf, including but not limited to Aditya Jain.

DOCUMENTS TO BE PRODUCED

1. All Documents and Communications from 2014 to 2020 related to Plaintiff Farhad Azima, including but not limited to Documents and Communications related to Plaintiff's Hacked Data.
2. All Documents and Communications from 2014 to 2020 related to work performed by you on behalf of Defendants, including invoices, bank records, engagement letters, scope of work, expense reports, reports, work product, and correspondence with Defendants.
3. All Documents and Communications from 2014 to 2020 related to any of the following individuals or entities:
 - a. CyberRoot Risk Advisory Private Limited ("CyberRoot");
 - b. BellTroX Info Tech Services ("BellTroX");
 - c. Aditya Jain or Jain Entities, including but not limited to Cyber DNA, Cyber DNA Labs, WhiteInt, and Arceus; or
 - d. NSO Group Technologies LTD ("NSO Group").

General Instructions:

Electronic files must be produced in their native format, i.e. the format in which they are ordinarily used and maintained during the normal course of business. For example, an MS Excel file must be produced as an MS Excel file rather than an image of a spreadsheet. (Note: An Adobe PDF file is not considered a native file unless the document was initially created as a PDF.)

If your production will be de-duplicated it is vital that you

1. preserve any unique metadata associated with the duplicate files, for example, custodian name, and,
2. make that unique metadata part of your production.

Data Delivery Standards

General requirements for ALL document productions are:

1. A cover letter should be included with each production and include the following:
 1. Case number
 2. A list of each piece of media included in the production with its unique production volume number
 3. A list of custodians, identifying the Bates range for each custodian.
 4. The time zone in which the emails were standardized during conversion.
2. Productions may be submitted via Secure File Transfer.
3. Alternatively, data can be produced on CD, DVD, thumb drive, hard drive, using the media requiring the least number of deliverables.
4. All submissions must be organized by custodian unless otherwise instructed.
5. All document family groups, i.e. email attachments, embedded files, etc., should be produced together and children files should follow parent files sequentially in the Bates numbering.
6. All load-ready collections should include only one data load file and one image pointer file.
7. All load-ready text must be produced as separate text files.
8. All load-ready collections should account for custodians in the custodian field.
9. Only alphanumeric characters and the underscore character are permitted in file names and folder names. Special characters are not permitted.
10. All productions must be produced using industry standard self-extracting encryption software.
11. All productions must be encrypted using a complex, unique password.
12. Passwords for electronic documents, files, compressed archives and encrypted media must be provided separately either via email or in a separate cover letter from the media.
13. All electronic productions should be produced free of computer viruses.

Delivery Formats

I. Concordance® Imaged Productions

All scanned paper and electronic file collections should be converted to TIFF files, Bates numbered, and include fully searchable text files.

1. Images
 - a. Black and white images must be 300 DPI Group IV single-page TIFF files.
 - b. Color images must be produced in JPEG format.
 - c. File names cannot contain embedded spaces or special characters (including the comma).

- d. Folder names cannot contain embedded spaces or special characters (including the comma).
- e. All TIFF image files must have a unique file name, i.e. Bates number.
- f. Images must be endorsed with sequential Bates numbers in the lower right corner of each image.
- g. The number of TIFF files per folder should not exceed 1,000 files.
- h. Excel spreadsheets should have a placeholder image named by the Bates number of the file.
- i. AUTOCAD/photograph files should be produced as a single page JPEG file.

2. Concordance Image® OR Opticon Cross-Reference File

The image cross-reference file (.LOG or .OPT) links the images to the database records. It should be a comma-delimited file consisting of seven fields per line with a line in the cross-reference file for every image in the database with the following format:

ImageID,VolumeLabel,ImageFilePath,DocumentBreak,FolderBreak,BoxBreak,PageCount

3. Concordance®Data File

The data file (.DAT) contains all of the fielded information that will be loaded into the Concordance® database.

- a. The first line of the .DAT file must be a header row identifying the field names.
- b. The .DAT file must use the following Concordance® default delimiters:
Comma ASCII character (020)
Quote ¨ ASCII character (254)
- c. Date fields should be provided in the format: mm/dd/yyyy
- d. Date and time fields must be two separate fields.
- e. If the production includes imaged emails and attachments, the attachment range must be included to preserve the parent/child relationship between an email and its attachments.
- f. A TEXT LINK field must be included to provide the file path and name of the extracted text file on the produced storage media. The text file must be named after the BEGDOC. Do not include the text in the .DAT file.
- g. For productions with native files, a NATIVE LINK field must be included to provide the file path and name of the native file on the produced storage media. The native file must be named after the BEGDOC.
- h. BEGATT and ENDAT fields must be two separate fields.
- i. A complete list of metadata fields is available as a separate attachment.

4. Text

Text must be produced as separate text files, not as fields within the .DAT file. The full path to the text file (TEXT LINK) should be included in the .DAT file. We require document level text files, named per the BEGDOC/Image Key. Extracted text files must be in a separate folder, and the number of text files per folder should not exceed 1,000 files. There should be no special characters (including commas in the folder names). For redacted documents, provide the full text for the redacted version.

5. Linked Native Files

Copies of original email and native file documents/attachments must be included for all electronic productions.

- a. Native file documents must be named per the BEGDOC number.
- b. The full path of the native file must be provided in the .DAT file for the NATIVE LINK field.
- c. The number of native files per folder should not exceed 1,000 files.

II. Adobe PDF File Production

With prior approval, Adobe PDF files may be produced in native file format.

1. PDF files should be produced in separate folders named by the custodian. The folders should not contain any special characters (including commas).
2. All PDFs must be unitized at the document level, i.e., each PDF must represent a discrete document.
3. All PDF files must contain embedded text that includes all discernible words within the document, not selected text or image only. This requires all layers of the PDF to be flattened first.
4. If PDF files are Bates endorsed, the PDF files must be named by the Bates range.